IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

ELIZABETH SINES, et al.,	)	Case No. 3:17-cv-00072-NKM-JCH
	)	
Plaintiffs,	)	
	)	
v.	)	
	)	
JASON KESSLER., et al.,	)	
	)	
Defendants.	)	
	)	
	)	
	)	

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF JOHN DOE'S MOTION TO QUASH SUBPOENAS TO TWITTER, INC., GODADDY.COM LLC, CLOUDFLARE, INC., AND HATREON

I. INTRODUCTION

Plaintiffs have made this Court a participant in 21st Century McCarthyism. Relying on the tenuous conspiracy theories plead in their Complaint(s), Plaintiffs have served sweeping third party subpoenas on a number of internet service providers calculated to uncover the anonymous identities of tens, if not hundreds of thousands, of individuals whose only fault is some affiliation with a political movement with which Plaintiffs' counsel disagree. If allowed, Plaintiffs' third party discovery will chill legal political speech and discourage political association in contravention of the First Amendment. Indeed, to silence right wing speakers, embarrass and deny livelihoods to their followers, and to break up right wing political organizations appears to be the entire point, not just of the subject third party discovery, but of this underlying lawsuit as well. The Court should decline to exercise its power in support of Plaintiffs' unconstitutional witch-hunt.

Pursuant to Federal Rule of Civil Procedure 45(d), 26(c) and 18 U.S. Code § 2702, Non-Party John Doe Movant hereby moves to quash Plaintiffs' subpoenas issued by counsel for Plaintiffs from this Court on or around January 30 through February 1, 2018 to Twitter, Inc., Godaddy.com LLC, Cloudflare, Inc., and Hatreon. Doc. 226-2 - 226-5[1]. These subpoenas seek identifying information for likely tens of thousands of non-parties, and perhaps many more, who have no connection whatsoever to the August 12, 2017 "Unite the Right" rally in Charlottesville, VA. Plaintiffs' discovery seeks to sweep up and unmask these people merely because they may have communicated via Twitter with, or about, a named defendant or alleged "co-conspirator", funded political internet content or activism, or visited a political website. The true goal of the subpoenas appears to be the targeting of innocent people for harassment, professional retaliation, and possible physical harm because of their anonymous political speech and political associations. But these activities stand at the very heart of the First Amendment, are strongly protected, and Plaintiffs' cannot clear the high relevance bar necessary to overcome those First Amendment protections. Additionally, since the Twitter and Hatreon subpoena seeks the production of electronic *communications*, as well as records, Twitter and Hatreon's compliance with the subpoena is barred under 18 U.S. Code § 2702(a)(1). Finally, the subpoenas' requests are staggeringly overbroad, and would fail Fed. R. Civ. P. 26's proportionately requirements, even if they weren't already fatally defective on constitutional and statutory grounds. All four subpoenas should be quashed in their entirety.

[1] All "Doc" citations are to the instant case's ECF docket.

II. STATEMENT OF FACTS

A. Plaintiffs' Subpoenas.

1. The Twitter Subpoena.

"Twitter is a social networking service that permits users to post [] messages using short communications called 'tweets,' and to read the tweets of other users. Users can monitor, or 'follow,' other users' tweets, and can permit or forbid access to their own tweets. In addition to posting their own tweets, users may send messages to a single user ("direct messages") or repost other users' tweets ('retweet'). " *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. sec. 2703(d)*, 830 F. Supp. 2d 114, 118, 2011 WL 5508991 (E.D. Va. 2011). Unless a Twitter user has "blocked" or "muted" another specific Twitter user, anyone may see anyone else's tweets, and may respond to them or retweet them to their own followers. See https://help.twitter.com/en/using-twitter#blocking-and-muting; https://help.twitter.com/en/using-twitter/mentions-and-replies.

Counsel for Plaintiffs signed a subpoena directed to Twitter on January 30, 2018. Doc. 226-2 at 10. The Twitter subpoena seeks production of documents related to "Primary Users" and "Secondary Users". *Id.* at 5. "Primary Users" appear to be Twitter accounts related directly to named Defendants or alleged co-conspirators, e.g., @RichardBSpencer and @DrDavidDuke. *Id.* The subpoena defines "Secondary Users" as "any [Twitter] User that communicated with the Primary Users between June 1, 2017 and August 18, 2017." *Id.* "Communication" and "communications" are defined broadly "to include any tweet or direct message on Twitter", and the subpoena further provides that "[a] communication is considered sent to a Twitter handle when it includes that Twitter handle." *Id.* at 3 & 5. This would include both replying to a tweet

from a Twitter handle, and retweeting the tweet from the Twitter handle to one's own followers, since both actions would include the original Twitter handle.

Request No. 6 seeks "all documents and data sufficient to identify the accounts of all Secondary Users", where "account" refers to apparently all "data associated with a Twitter handle, including the Twitter handle following, the Twitter handle it follows, *tweets from that Twitter handle*, the timeline associated with that Twitter handle, *the direct messages associated with the Twitter handle*, and any data such as the user name, location, or associated website for that Twitter handle." *Id.* at 9 & 4-5 (emphasis added). Thus, under to the definitions set forth in the Twitter subpoena, Request No. 6 seeks the user name, location and other data associated with any Twitter user who either responded to or retweeted a tweet including the twitter handle of any Primary User within the specified timeframe, *regardless of the subject matter of the tweet*. Thus, any account that posts even a critical reply to one of the Primary Users is swept up in Plaintiffs' Request. Moreover, the accounts to be identified in response to Request No. 6 include accounts that merely "mention" one of the "Primary Users" - they are not limited to accounts that directly receive tweets from or directly tweeted to a "Primary User". This means that twitter handles that are engaged in discussions about, for example, @RichardBSpencer, or reply to people who replied to the @RichardBSpencer handle are "Secondary Users", which must be identified in response to Request No. 6[2]. Additionally, "identification" of Secondary Accounts under the subpoena includes not just records about the account (e.g., handle, user name, etc.), but also the *content* of both tweets and private direct messages themselves. Significantly, Request No. 6,

[2] For perspective on the scope of this Request, defendant Richard Spencer has over 80,000 Twitter followers as of February 19, 2018. See https://twitter.com/RichardBSpencer?lang=en. Any of those 80,000 people who replied to or re-tweeted a tweet from @RichardBSpencer between June 1, 2017 and August 19, 2017 is a "Secondary User" under the Twitter subpoena. Doc. 226-2 at 5 (paragraphs 20-21).

incorporating the broad definition of "account", seeks disclosure of all non-public direct messages with *any party whatsoever*, so long as those direct messages are associated with an associated "Secondary User". See Doc. 226-2 at 4-5. This request for all communications associated with a Secondary User is not limited in time or subject matter. *Id.*

Request No. 7 seeks "[a]ll communications between or among the Primary and Secondary Users between June 1, 2017 and August 19, 2017". By its terms, and under the definitions provided, Request No. 7 seeks all communications, including non-public direct messages, on whatever subject, including communications only between Secondary Users, in which no Primary User is involved.

2. The Godaddy Subpoena.

Godaddy is an internet domain name registrar and hosting service located in Scottsdale, Arizona. See *Koenig v. ALL.COM*, No. 1:08-CV-1169 (GBL), 2009 WL 2447945, at *2 (E.D. Va. July 31, 2009). Counsel for Plaintiffs signed the Godaddy subpoena on February 1, 2018. Doc. 226-3 at 8. Request No. 2(b) of the Godaddy subpoena seeks, *inter alia*, "[a]ll traffic logs for the Daily Stormer website from August 1 to 19, 2017, including all identifying information for each visitor to the Daily Stormer website such as timestamp, location, IP address and MAC address." *Id.* at 7. Request No. 3(b) seeks, *inter alia*, "[a]ll traffic logs for AltRight.com from August 1 to 19, 2017, including all identifying information for each visitor to AltRight.com such as timestamp, location, IP address and MAC address." *Id.* at 8.

3. The Cloudflare Subpoena.

Cloudflare is a distributed internet domain name server and security company located in San Francisco, California. See https://en.wikipedia.org/wiki/Cloudflare#Reverse_proxy. Cloudflare acts as a "reverse proxy", which means that Cloudflare's servers act as intermediaries

between web clients (e.g., users on the Internet searching for resources) and web servers (e.g., web sites hosting content). *Id.* This allows Cloudflare to detect and mitigate "distributed denial of service attacks", which seek to shut down a web server by rapid, repeated queries. *Id.* Counsel for Plaintiffs signed the Cloudflare subpoena on February 1, 2018. Doc. 226-4 at 9. Request No. 2(b) of the Cloudflare subpoena seeks, *inter alia*, "[a]ll traffic logs for the Daily Stormer website from August 1 to 19, 2017, including all identifying information for each visitor to the Daily Stormer website such as timestamp, location, IP address and MAC address." *Id.* at 7. Request No. 3(b) seeks, *inter alia*, "[a]ll traffic logs for AltRight.com from August 1 to 19, 2017, including all identifying information for each visitor to AltRight.com such as timestamp, location, IP address and MAC address." *Id.* at 8. Request No. 4(b) seeks, *inter alia*, "[a]ll traffic logs for the Right Stuff website from August 1 to 19, 2017, including all identifying information for each visitor to the Right Stuff website such as timestamp, location, IP address and MAC address." *Id.* at 9.

4. The Hatreon Subpoena.

Hatreon.com is an anonymous funding platform through which interested individuals can fund the creation of internet content (art, essay writing, videos, audio podcasts, etc.) from other people, or support their activism or other activities. See https://en.wikipedia.org/wiki/Hatreon. Hatreon was founded as a response to similar crowdfunding platforms (e.g., Patreon.com, Kickstarter.com, etc.) refusing to serve right-wing internet content creators by implementing strict policies regarding so-called "hate speech"). See *Id.* Plaintiffs' counsel signed the Hatreon subpoena on January 31, 2018. Doc. 226-5 at 9. Request No.1 to the Hatreon subpoena seeks all documents and communications regarding funding of any "Defendant or Other Relevant Individuals" including, *inter alia*, the identity of the sender and the recipient and transaction

records, dollar amount, payment method used, including the sender's bank or other financial accounts. *Id.* at 8. The list of "Relevant Individuals" includes over 50 individuals and organizations, most of whom are not named in Plaintiffs' Complaints either as Defendants or alleged co-conspirators. Request No. 2 seeks documents sufficient to show "the identity of any person or entity who contributed funds to any Defendants or Other Relevant Individuals, including such person or entity's name, user name, email address, phone number, mailing address, IP address, and MAC address." *Id.* at 8. Request Nos. 1 and 2 are not limited in time, and are not limited to the subject matter of the content or activity allegedly funded. Request No. 3 seeks all documents and communications concerning any solicitation or receipt of funds by any person relating to "costs related to the travel to, attendance at, lodging for, or legal fees arising from" a variety of rallies held in Charlottesville, VA. *Id.*

B. The Subpoenas Will Uncover Non-public Communications And Other Personally Identifying Information Of Non-Parties.

The information Plaintiffs seek will enable them to unmask the names of likely thousands of non-party individuals, generate information about their political persuasion and online reading habits, learn who they are conversing with online and about which subjects, and possibly to track their locations over time. Movant is specifically subject to these risks in the event that subpoenas are not quashed.

As is set forth in section II(A)(1) *supra*, the Twitter subpoena casts a wide net for "Secondary Users", defining those individuals as anyone who tweeted anything including the handle of a Primary User during a specified timeframe. Doc. 226-2 at 5. Then, for all Secondary Users, Request No. 7 demands all communications between a Primary User and a Secondary User, on whatever subject, during a specified time period (Doc. 226-2 at 9) and all communications occurring only between Secondary Users, on whatever subject, during the

specified timeframe (See *Id.*, "among..Secondary Users"). Worse, Request No. 6 seeks identification of all Secondary User accounts, where this is defined as production all data concerning the account including all tweets associated with the handle, and all non-public direct messages associated with the handle, to whatever party, on whatever subject. Doc. 226-2 at 4-5, definition of "account"). In other words, the Twitter subpoena requires turning over a Secondary User's entire Twitter direct message inbox just because the User may have retweeted a tweet from a Primary User account during the specified timeframe.

In addition to non-public communications, the Twitter subpoena seeks personally identifying information about untold thousands of users. See e.g., Doc. 226-2 at 9 (Request No. 6) & 4-5 (defining "account" to include user name, location, and "any [other] data...for that Twitter handle."). A Twitter user name may be associated with an individual's actual name, but more to the point, Twitter requires an email address to register, and for certain accounts, requires a telephone number for verification. See https://help.twitter.com/en/managing-your-account#username-email-and-phone, under the headings "username, email and phone". Under the Twitter subpoena's broad definition of "account", this email and telephone data would be produced. Telephone numbers are clearly personally identifying, and email addresses may be personally identifying, particularly if they include a person's actual name, or are associated with other email addresses that do. The Requested location information (i.e., the location from which a person submitted a tweet), may also be used to track an individual's movements, and may be correlated with other data about that individual to reveal their identity.

The Cloudflare and Godaddy supoenas seek traffic logs (i.e., logs of information about visiting computer connections) including the time stamp, location of the requesting client, IP addresses and MAC addresses of connecting computers for three websites: Altright.com, The

Daily Stormer and The Right Stuff. Doc. 226-3 at 7-8; Doc. 226-4 at 7-9. Information responsive to these Requests will allow Plaintiffs to build a database of the location, IP address and MAC address of every Internet user who visited one of the subject websites during a specified timeframe. There is a wealth of individually identifying information in the traffic logs that are subject to these Requests.

An IP address is a numeric value used to identify the network location of a computer or set of computers on the Internet. See https://en.wikipedia.org/wiki/IP_address. Internet routers use the IP address to decide where to send communications addressed to a particular computer user. *See Id.* IP addresses are allocated to Internet service providers (e.g., Comcast, Verizon, and business or enterprise ISPs) and often reflect the general physical location of the area they serve, and in any event, the physical location of an ISP's IP address is generally publicly available information that can be found on the Internet. See, e.g., https://whatismyipaddress.com/; http://geobytes.com/. Even where an IP address is not publicly related to a physical location, a subpoena to the ISP can reveal the physical location associated with an individual subscriber IP address to the level of the subscriber's physical address. ISP's can also delegate IP addresses to other entities like businesses, Universities, or smaller ISPs, and these delegated IP addresses can be used to identify those entities. MAC addresses, also being requested, are unique, individual identifiers associated with a network interface controller for a specific machine (e.g., one's laptop, smart phone, or home router or gateway). See https://en.wikipedia.org/wiki/MAC_address.

Having access to all of the information would allow Plaintiff to do a number of things. First, traffic logs such as those Requested by Plaintiffs can be used to locate the physical location, at least roughly, of a unique individual visitor to a website, and specific location data

can be had through further discovery directed at an individual's ISP, once the visiting IP address is in hand. Indeed, Plaintiffs' Requests explicitly ask for the "location" of the visiting computers in their definitions of "traffic logs". Second, the traffic logs, in some cases, can identify the computer system the individual user is using to visit the subject website, e.g., the identity of the university system being used, or possibly the individual's employer in the event that a business system is being used. Third, by also asking for MAC addresses, the requested traffic logs can be used to build a map of movements of particular individuals over time. For example, if someone visits Altright.com using their phone logged into WiFi at a University ISP, then later visits the same site from her home network, then later goes on a trip and visits the same site using her phone from an internet café's Wifi, the traffic log will reveal the phone's movement over time. By comparing this sort of information with timestamp information (also requested), and by comparing patterns among different devices, the requested traffic logs can also reveal meetings between individuals in various places over time.

More direct personally identifying information is sought in the Hatreon subpoena, which asks for names, email addresses, phone numbers, and IP addresses for anyone who contributed funds through Hatreon, at whatever time and for whatever purpose, to any named Defendant or anyone else in a list of over 50 individuals. Doc. 226-5 at 8.

C. Movant's Non-Public Communications And Personally Identifying Information Will Be Divulged In Response To The Subpoenas, Putting Movant At Risk Of Harm

As is set forth in the Declaration of John Doe, Movant's non-public Twitter communications and other personally identifying information will be divulged in response to the subpoenas. If Movant's advocacy of ideas associated with the "alt-right" becomes publicly

known, Movant will suffer personal and professional consequences, which consequences will tend to discourage Movant's political speech, advocacy and association.

Movant engages in online anonymous political speech and advocacy through Movant's Twitter account. Doe Dec., ¶¶4-5. Movant does this by posting to Twitter, and by exchanging direct messages with other Twitter users who are like-minded. *Id.* at ¶¶5-6. Between June 1, 2017 and August 17, 2017, Movant replied on Twitter to a tweet posted by one of the "Primary User" accounts listed in the Twitter subpoena. *Id.* at ¶7. Movant is therefore a "Secondary User" under the Twitter subpoena. *Id.* Movant's Twitter handle is pseudonymous, but Movant's Twitter account is associated with Movant's phone number and an email account, which itself is associated with another email account incorporating Movant's true name. *Id.* at ¶4. Thus, Movant's phone number is directly responsive to the Twitter subpoena, and the email account associated with Movant's Twitter account can be used, with further discovery on Movant's email service providers, to reveal Movant's name. See *Id.*

Additionally, Movant visits the websites for which the subpoenas seek traffic logs. Doe Dec. at ¶¶8-9. Most of these visits are to the Right Stuff website, which Movant visits primarily to listen to political and cultural podcasts. ¶9. Movant also posts to a user forum at the Right Stuff website. *Id.* These posts are generally about political or cultural issues of the day. *Id.* Movant is certain that Movant visited the Right Stuff website between August 1 and August 19, 2017. *Id.* Accordingly, information regarding Movant's visit to the Right Stuff website would be produced in traffic logs for the Right Stuff website, if any exist. See *Id.*

Movant also has a Hatreon account, which Movant established to anonymously support essayists and podcast producers whose work Movant enjoys, and political activists with whom Movant agrees. See Doe Dec. at ¶10. Movant's Hatreon account is associated with an email

account, which itself is associated with another email account incorporating Movant's true name. *Id.* Movant does not believe that Movant actually donated any money through Hatreon.

Movant is concerned that the information sought by the subpoenas will reveal Movant's true identity and online associations with "alt-right" people and advocacy for their ideas. Doe Dec. at ¶¶ 3 & 11. Movant is worried that Movant will suffer personally and professionally in the event that Movant's identity is revealed by Plaintiffs' discovery. *Id.* at ¶¶ 11-12. Specifically, Movant fears that, if Movant is identified in connection with this litigation, Movant's familial relations will be strained, Movant will be socially ostracized, and that Movant will lose Movant's job. *Id.* This fear is based on well publicized stories of the negative personal and professional consequences suffered by other people in the "alt-right", whose identities have been revealed. *Id.* at ¶11. Additionally, Movant fears physical harm to Movant and Movant's family in the event that Movant is personally identified. *Id.* at ¶13. This fear is based on news stories regarding "alt-right" figures who have been attacked, such as Richard Spencer. *Id.*

Being personally identified is highly likely to cause Movant to engage in less political expression, advocacy and association. See Doe Dec. at ¶14. In fact, fear of being personally identified through Plaintiffs' subpoenas has already caused Movant to be less active in online political discussions and advocacy. *Id.* Movant associates less online with people in the "alt-right" than Movant used to. Movant is unwilling to donate to activists and content providers on the "alt-right" for fear of being personally identified. *Id.*

III. LEGAL STANDARD

The Federal Rules of Civil Procedure permit the discovery of "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1). A party seeking discovery that implicates the First Amendment rights of

freedom of speech or association, however, must show that "information sought is *highly relevant* to the claims or defenses in the litigation—a more demanding standard of relevance than that under Federal Rule of Procedure 26(b)(1)." *Perry v. Schwarzenegger*, 591 F.3d 1126, 1141 (9th Cir. 2010) (emphasis added). Additionally, even if allowed, discovery implicating First Amendment rights must be "carefully tailored to avoid unnecessary interference with protected activities, and the information must be otherwise unavailable." *Id.* A court must quash or modify a subpoena if it "requires disclosure of privileged or other protected matter" or "subjects a person to undue burden." Fed. R. Civ. P. 45(d)(3)(A)(iii), (iv). A court may quash a subpoena *sua sponte*, even if it determines that a party or non-party lacks standing to bring a motion to quash. See *Jefferson v. Biogen IDEC Inc.*, No. 5:11-CV-00237-F, 2012 WL 1150415, at *2 (E.D.N.C. Apr. 5, 2012); *Newcomb v. Principal Mut. Life Ins. Co.*, No. 1:07cv345, 2008 U.S. Dist. LEXIS 79980, at *8, 2008 WL 3539520 (W.D.N.C. Aug. 11, 2008) (denying the plaintiff's motion to quash the defendant's subpoena where the plaintiff lacked standing but nevertheless *sua sponte* quashing the subpoenas as outside the bounds of Rule 26(b)(4)(A)).

Additionally, the Stored Communications Act (18 U.S.C. §2701 et seq.) prohibits the release of stored electronic communications in response to a civil subpoena. *In re Subpoena Duces Tecum to AOL*, LLC, 550 F.Supp.2d 606, 611 (E.D. Va. 2008).

Finally, a court may quash a subpoena if it is overbroad or seeks irrelevant information. *Singletary v. Sterling Transp. Co.*, 289 F.R.D. 237, 241, 2012 WL 5449687 (E.D. Va. 2012) citing *Cook v. Howard*, No. 11–1601, 2012 WL 3634451, at *6 (4th Cir. Aug. 24, 2012) (per curiam) ("Although Rule 45(c) sets forth additional grounds on which a subpoena against a third

party may be quashed ... those factors are co-extensive with the general rules governing all discovery that are set forth in Rule 26.").

IV. ARGUMENT

A. The Subpoenas Violate Movant's First Amendment Rights

The subpoenas should be quashed in their entirety because they violate Movant's First Amendment rights to anonymous speech and association. The Court should subject these subpoenas to particular scrutiny because production will chill political speech about and associations concerning important issues of the day - the sort of activity that lies at the very heart of the First Amendment's protection. *Meyer v. Grant*, 486 U.S. 414, 422, 425 (1988) (describing the First Amendment protection of "core political speech" to be "at its zenith").

1. Movant has a First Amendment privilege to engage in anonymous political speech.

The First Amendment guarantees the right, not only to organize and engage in political advocacy and debate, but also the right to do so anonymously. Where discovery seeks identifying information about speakers engaged in such activity, the party seeking discovery bears the burden of demonstrating a compelling need for the identifying information. Plaintiffs here cannot carry this burden.

a. The First Amendment protects the right to engage in anonymous speech.

The Anglo-American tradition of anonymous political speech pre-dates the founding of the Republic. As Justice Black noted, writing for the Supreme Court almost 60 years ago,

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies was due in part to the knowledge that exposure of the names of printers, writers and distributors would

> lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get evidence to convict him or someone else for the secret distribution of books in England. Two Puritan Ministers, John Penry and John Udal, were sentenced to death on charges that they were responsible for writing, printing or publishing books. Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. Along about that time the Letters of Junius were written and the identity of their author is unknown to this day. Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.

Talley v. California, 362 U.S. 60, 64–65 (1960) (striking down a California law banning the distribution of handbills that did not include the name and address of the author.). On similar facts to those in *Talley*, the Court struck down another statue barring anonymous political handbills in 1995, stating,

> The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.

McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995). Anonymous tweets and other Internet postings should be thought of as the 21st century version of anonymous political handbills, or the anonymously published Federalist pamphlets. And indeed, courts have found that the First Amendment's protections for anonymous speech extend beyond political flyers to email messages and Internet message board postings like the ones sought here. See *Reno v. ACLU*, 521 U.S. 844, 870 (1997); *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) ("The right to speak anonymously extends to speech via the Internet. Internet

anonymity facilitates the rich, diverse, and far ranging exchange of ideas."). A court order such as a subpoena constitutes state action implicating these Constitutional protections, even in the context of private civil litigation. *See, e.g., New York Times v. Sullivan*, 376 U.S. 254, 265 (1964); *Shelley v. Kraemer*, 334 U.S. 1, 14 (1948).

b. Anonymous speakers enjoy a limited privilege under the First Amendment.

Because the First Amendment protects anonymous speech and association, those engaged in anonymous speech and association enjoy a qualified privilege to resist state efforts to pierce their anonymity, including discovery orders such as subpoenas. In recognition of this privilege, courts must "be vigilant . . . [and] guard against undue hindrances to . . . the exchange of ideas." *Buckley v. Am. Constitutional Law Found.*, 525 U.S. 182, 192 (1999). Just as in other cases in which litigants seek information that may be privileged, courts **must** consider the privilege before authorizing discovery. See, e.g., *Sony Music Entm't Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 565 (S.D.N.Y. 2004) ("Against the backdrop of First Amendment protection for anonymous speech, courts have held that civil subpoenas seeking information regarding anonymous individuals raise First Amendment concerns."); *Grandbouche v. Clancy*, 825 F.2d 1463, 1466 (10th Cir. 1987) (citing *Silkwood v. Kerr-McGee Corp.*, 563 F.2d 433, 438 (10th Cir. 1977)) ("[W]hen the subject of a discovery order claims a First Amendment privilege not to disclose certain information, the trial court must conduct a balancing test before ordering disclosure.").

This careful balancing between the need for the discovery and the First Amendment chilling effect the discovery will have is particularly critical in circumstances like this one, where the discovery is aimed squarely at chilling *political* speech and association on the Internet. As the Northern District of California observed almost two decades ago "[p]eople who have committed no wrong should be able to participate online without fear that someone who

wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity." *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

Here, Plaintiffs are seeking personally identifying information about Movant, as well as likely thousands of others of individuals, through its Requests. As is set forth in Section II *supra*, the Twitter subpoena seeks all information associated with Movant's Twitter account, which includes Movant's user name, location, email address, phone number, and all non-public direct messages associated with Movant's account. This information made be used to reveal Movant's personal identity. The Godaddy and Cloudflare subpoenas seek the IP addresses and locations from which Movant visited certain websites, and the MAC addresses of whatever machines Movant may have used during those visits - information that provides additional information useful to revealing Movant's identity including information, potentially, about Movant's location, employer (in the case of a Business IP domain) or university (in the case of a University IP domain).

The consequences for personal identification would be severe, for Movant, as well as for all the other innocent third parties swept up in Plaintiffs' proposed dragnet. Far-right politics are deeply unpopular in the United States, earning the support of only 10% of Americans. See http://abcnews.go.com/Politics/28-approve-trumps-response-charlottesville-poll/story?id=49334079. Members of the far right who are "doxed"[3] quickly find themselves

[3] See https://en.wikipedia.org/wiki/Doxing (defining doxing as the revelation of a person's anonymous online identity).

unemployable[4], divorced or disowned by their families[5], facing calls for expulsion from school[6], and the victims of physical assault[7]. Indeed, the extra-judicial punishment meted out to people for holding far-right views has become so normalized that the New York Times even ran an article seriously asking "Is it OK to punch a Nazi [sic]"[8].

The constitutional privilege to remain anonymous certainly has limits. For example, it may not be used to shield anonymous internet users from liability for tortious acts such as defamation. *Columbia Ins. Co.*, 185 F.RD. at 587. However, Plaintiffs have not and cannot make any showing that the many thousands of Internet users targeted by the subpoenas are engaged in tortious activity merely because they have some tenuous online association with a named Defendant or alleged co-conspirator. Rather, Plaintiffs are simply using the discovery power to uncover the identities of people who may have made statements with which they disagree or associate with people whom they dislike. This, the Constitution does not permit, and accordingly, courts evaluating attempts to unmask anonymous speakers in cases similar to the ones at hand have adopted standards that balance one person's right to speak anonymously with a litigant's legitimate need to pursue a claim.

An instructive case suggesting proper First Amendment restrictions upon a litigant's ability to compel an online service provider to reveal an anonymous non-party's identity

---

[4] See http://www.foxnews.com/us/2018/01/06/maryland-substitute-teacher-fired-after-alt-right-views-discovered-by-students.html

[5] See https://www.dailydot.com/layer8/pete-tefft-father-letter-to-the-editor/

[6] See http://www.newsweek.com/university-nebraska-wont-expel-student-who-boasted-being-most-active-white-802720

[7] See https://www.cnn.com/2017/01/20/politics/white-nationalist-richard-spencer-punched/index.html.

[8] See https://www.nytimes.com/2017/01/21/us/politics/richard-spencer-punched-attack.html

is *Doe v. 2theMart.com*[9], *supra*, in which the Western District of Washington adopted a four-part test for protecting anonymous speakers. This test has been followed by courts around the country[10], and it should be adopted here. Under the *2theMart* framework, in order for the litigant to obtain the anonymous non-party's identity, he must show:

> (1) the subpoena seeking the information was issued in good faith and not for any improper purpose,
>
> (2) the information sought relates to a core claim or defense,
>
> (3) the identifying information is directly and materially relevant to that claim or defense, and
>
> (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source.

2theMart.com, 140 F. Supp. 2d at 1095. In setting forth the test, the *2theMart.com* court warned that "non-party disclosure is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker." *Id.*

While *2theMart.com* provides a useful framework, other courts have set the bar far higher. In considering a request to unmasked anonymous speakers engaged in political speech, the Delaware Supreme Court in *Doe v. Cahill*, 884 A.2d 451 (Del.2005) required plaintiffs to be able to survive a hypothetical motion for summary judgment and give, or attempt to give, notice to each anonymous speaker to object before discovering the anonymous speaker's identity. *Id.* at 461. The 9th Circuit, and other courts, have noted that *Cahill*'s more exacting requirements are appropriate in circumstances such as this one, where the anonymous speakers are engaged in political speech. *In re Anonymous Online Speakers*, 661 F.3d 1168, 1176–77 (9th Cir. 2011);

---

[9] Cited with approval by this Court's sister court in *Taylor v. John Does 1-10*, No. 4:13-CV-218-F, 2014 WL 1870733, at *2 (E.D.N.C. May 8, 2014).

[10] *See, e.g., Enterline v. Pocono Medical Center*, 751 F. Supp. 2d 782, 787 (M.D. Pa. 2008); *Mobilisa, Inc. v. Doe*, 170 P.3d 712, 719 (Ariz. App. 2007).

Taylor, 2014 WL 1870733 at *2 ("The degree of First Amendment protection afforded the particular speech at issue should be a driving force in choosing a standard by which to balance the rights of anonymous speakers [with the rights of aggrieved parties].") (internal quotation omitted). Whichever standard the Court selects, either *Cahill*'s stricter standard, or *2theMart*'s more permissive one, Plaintiffs fail to meet it.

c. Plaintiffs Cannot Make The Showing Required Under The *2theMart* Framework.

i. The Subpoenas Are Brought For An Improper Purpose.

Plaintiffs' subpoenas have not been issued for the purpose of building a case to redress the wrongs suffered by the Plaintiffs at Charlottesville on August 12, 2017. Rather, the goal of these subpoenas is to chill far-right speech and association by publicly identifying, shaming and blacklisting anyone who even tangentially associates themselves with far-right politics. The end game is simple - to identify anyone who has ever communicated with, about or consumed content produced by a named defendant or alleged co-conspirator, or other like-minded people, in an ever growing dragnet, and then once they have been identified, to make all those people unemployable, to destroy their family relations and to cast them out of polite society forever. This has been a favored tactic used by the powerful to crush political dissidents. It was the tactic used during the Red Scare of the 1950s; it was the tactic attempted against organizations like the

NAACP[11], the Black Panthers[12] and various environmental advocacy and labor organizations[13], and it is the same tactic being used here.

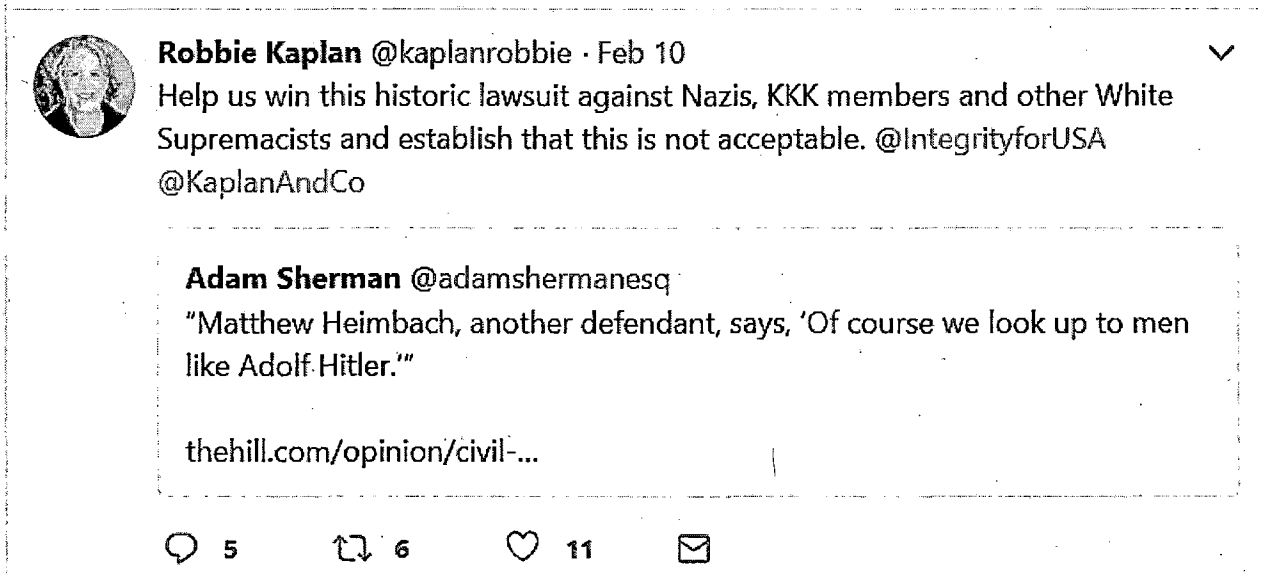
We know this for two reasons. First, the scope of the subpoena Requests goes well beyond what would be required to support Plaintiffs' claims. The gravamen of Plaintiffs' case is that over two dozen individuals and organizations conspired to incite violence at the August 12, 2017 Unite the Right rally. In view of that theory, discovery directed to the communications of those individuals might be appropriate, depending on the subject matter of those communications. But the subpoenas go well beyond that. The subpoenas seek identifying information and communications from untold thousands of people whose only offense may have been to be one of Defendant Richard Spencer's 80,000 Twitter followers, or to have read an irreverent and satirical article at The Daily Stormer, or to have listened to a movie review podcast[14] or a cooking podcast[15] on The Right Stuff website. The breadth of the subpoena Requests themselves indicates that the subpoenas have not been issued in good faith.

Second, we know that the subpoenas are issued for an improper purpose, because counsel for Plaintiffs have said as much. On February 10, 2018, for example, lead counsel for Plaintiffs, Roberta Kaplan retweeted a quote from defendant Matthew Heimbach[16], and asked her Twitter

---

[11] See *NAACP v. State of Alabama ex rel. Patterson*, 357 U.S. 449, 460-66 (1958) (overturning state Court order requiring production of the NAACP's membership list.)
[12] See *Black Panther Party v. Smith*, 661 F.2d 1243, 1267-68 (D.C. Cir. 1981) (upholding litigant's refusal to produce membership list in response to discovery request).
[13] See, e.g., *Marfork Coal Co. v. Smith*, 274 F.R.D. 193, 205, 2011 WL 1044496 (S.D.W. Va. 2011) (denying discovery request directed to defendant environmental advocacy organization's member list).
[14] See e.g., https://therightstuff.biz/2018/02/13/the-poz-button-43-outlaw-josey-wales/
[15] See e.g., https://therightstuff.biz/2018/02/13/the-white-flour-hour-episode-7-iko-iko-iko/
[16] It is worth noting that had Ms. Kaplan retweeted a tweet directly from Mr. Heimbach's own apparent twitter account, @MatthewHeimbach, between June 1, 2017 and August 19, 2017, even to criticize Mr. Heimbach in this manner, Ms. Kaplan would be classified as a "Secondary User"

followers to fund the instant suit to "establish that this is not acceptable". The tweet[17] is pictured below:



In the quote, Mr. Heimbach appears to express some admiration for Adolf Hitler - a sentiment with which virtually all people would disagree. But it is not the proper purpose of litigation, or discovery requests served in connection with litigation, to render certain opinions, however unpopular, "unacceptable". But according to Plaintiffs' counsel, that is the goal of this lawsuit: to regulate the expression of unpopular political opinions like Mr. Heimbach's. Ms. Kaplan's public admission compels the conclusion the subject discovery is brought for an improper purpose.

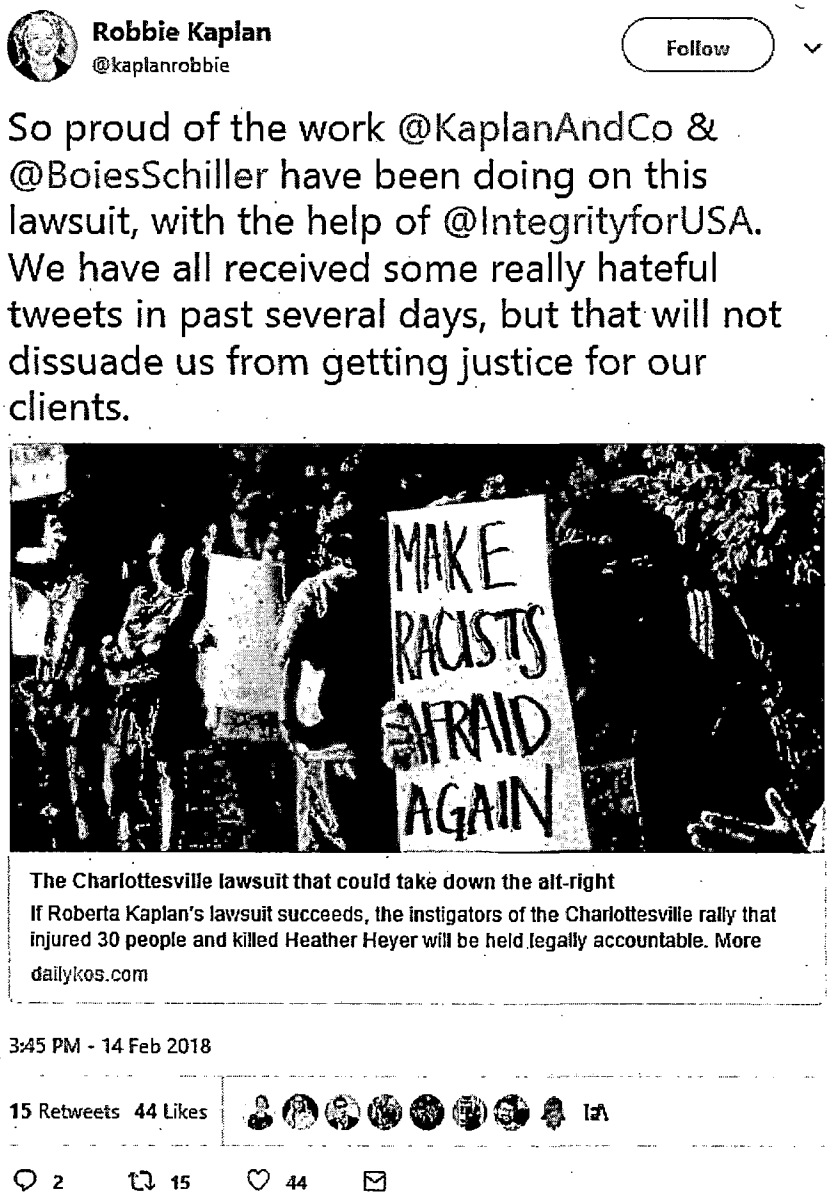
Worse still, on February 14, 2018, Ms. Kaplan sent out a tweet[18] to her followers referencing co-counsel Boies Schiller and this litigation. The tweet contained an image of a protest sign reading "Make Racists Afraid Again." The tweet is pictured below:

---

under the Twitter subpoena, and her entire Twitter timeline and direct message inbox would be subject to production. See 226-2 at 4-5 & 9.

[17] See https://twitter.com/kaplanrobbie/status/962306337655939074

[18] See https://twitter.com/kaplanrobbie/status/963922141866549248



Now, had any one of the named individual Defendants retweeted a message like "Make [Whichever Group] Afraid Again" that would have been presented as evidence in Plaintiffs' Complaint for a conspiracy to incite violence against the mentioned group. Even if one charitably assumes that Plaintiffs' counsel's tweet is not a threat of physical violence against Americans who share the political and cultural beliefs of the Defendants, it still reveals that this

litigation, and particularly this discovery, is brought for an improper purpose. The unmistakable message of Plaintiffs' counsel's tweet is that the goal of this case is not to make the Plaintiffs' whole, but rather, to make "racists" afraid. The subject subpoenas are the first step in that process - the first stage of a sweeping pogrom calculated to sow fear in thousands of people who stand at risk at being doxed, and having their lives ruined for doing nothing more than engaging in political debate, or reading right-of-center political and cultural content on the Internet.

This lawsuit's true goals are not a mystery to the interested public. Ms. Kaplan recently spoke to the New York Times about the instant suit[19]. After talking with Ms. Kaplan, the author of the Times piece, Alan Feuer, was left with the impression that "[d]iscovery in [this] case may also expose the links between the far-right groups and their often opaque sources of financing." The left-of-center political blog The Daily Kos, in the article retweeted by Ms. Kaplan above, went farther, saying "[i]f Roberta Kaplan's lawsuit succeeds…the alt-right's funding streams and structures will be exposed." But associating with far-right groups or financing them is not illegal, and discovery aimed at shutting down such activities, such as this discovery, is improper.

ii. The Information Sought By The Subpoenas Does Not Relate To A Core Claim And The Identifying Information Is Not Directly Or Materially Relevant To A Claim.

In order for Plaintiffs to obtain identifying third party information, they must show that the information requested relates to a core claim or defense and that the identity information is directly and material relevant to that claim or defense. See *2theMart.com*, 140 F. Supp. 2d at 1096. Plaintiffs cannot make this showing. It is impossible to say with precision how many individuals stand to have their anonymous data and communications disclosed under the

[19] See https://www.nytimes.com/2018/02/12/us/charlottesville-lawsuit-far-right-heather-heyer.html

subpoenas, but for perspective, the Twitter subpoena seeks all account information for anyone who replied to or retweeted a "Primary User" Twitter account between June 1 2017 and August 19, 2017, and for anyone who responded to or retweeted *those* people's tweets. Doc. 226-2 at 4-5 & 9 and see Section II(A)(1) *supra*. Primary User @RichardBSpencer currently has about 80,000 followers[20]. Primary User @DrDavidDuke currently has about 50,000 followers[21]. Primary User @IdentityEvropa currently has about 27,000 followers[22]. Those followers see every tweet originating from the accounts they follow, and are in a position to easily respond to those tweets, or retweet them, which creates a "communication", which identifies a "Secondary Account" under the Twitter subpoena. Doc. 226-2 at 5. And the examples above are just three of the twenty-four Primary User accounts mentioned in the Twitter subpoena. *Id.* The web of "Secondary Users" for which the Twitter subpoena seeks account information is likely in the high tens of thousands, if not more than one hundred thousand. And each of those accounts is likely to have generated thousands of tweets and direct messages during its history, all of which are sought by the Twitter subpoena. *Id.* at 4-5 (defining "account" to include timeline (i.e., all tweets sent by or posted to the account) and direct messages associated with the account). The number of individual tweets or messages responsive to the Twitter subpoena probably runs into the hundreds of thousands, if not millions.

The Requests for traffic logs under the Cloudflare and Godaddy subpoenas, including the IP and MAC addresses for every visitor, are similarly staggeringly overbroad. While Movant does not know the volume of internet traffic received at The Daily Stormer, AltRight.com or The Right Stuff, Thomas J. Main, professor at the Austin W. Marxe School of Public and

[20] See https://twitter.com/RichardBSpencer
[21] See https://twitter.com/DrDavidDuke
[22] See https://twitter.com/IdentityEvropa

International Affairs of Baruch College, City University of New York writing for the Los Angeles Times estimated that The Daily Stormer received 997,000 visits and 284,000 unique visitors between September 2016 to May 2017[23]. This is a rate of about 3,600 visitors a day (and about 1,000 unique visitors a day), which would translate into 69,000 visitors or about 19,000 unique visitors during the 19 day time period[24] for which The Daily Stormer traffic logs are sought. Considering the other websites for which traffic logs are sought, Plaintiffs are seeking to uncover the IP addresses, MAC address and locations of tens of thousands of people.

The chances are near zero that all this information, or even a fraction of a percent of it, is in any way relevant to Plaintiffs' claims, much less directly and materially relevant to those claims, or relevant to a core claim.

iii. Plaintiffs Have Made No Showing that the Information Sought Is Unavailable from Any Other Source.

In order for Plaintiffs to receive the Requested third party information, they must show that "the information [Plaintiffs] need[] to establish its defense is unavailable from any other source." See *2theMart.com*, 140 F. Supp. 2d at 1097. They cannot do so.

The gravamen of Plaintiffs' case is that over two dozen individuals and organizations conspired to incite violence at the August 12, 2017 United the Right rally. If Plaintiffs want to understand the scope of their alleged conspiracy, the focus should be on the party Defendants, through conventional party discovery, and that focus should be kept squarely on party communications to advance the alleged conspiracy. To the extent that relevant party communications involve non-parties, then Plaintiffs may have cause to seek further, targeted discovery relating to those non-parties, and maybe even add those non-parties to the case. But

[23] http://www.latimes.com/opinion/op-ed/la-oe-main-alt-right-audience-20170822-story.html
[24] See Doc. 226-3 at 7.

the First Amendment's right to speak anonymously prevents Plaintiff from hoovering up personal identifying information on thousands of innocent individuals in pursuit of their case. Plaintiffs cannot satisfy the *2theMart.com* test, and their subpoenas must be quashed because they violate Movant's First Amendment right to anonymity.

2. The Subpoenas Violate Movant's First Amendment Right to Association

Plaintiffs' subpoenas trammel upon the Movant's constitutionally guaranteed right to association. This alone requires that the subpoenas be quashed in their entirety.

a. Movant Has A First Amendment Right To Anonymous Political Association And To Anonymously Advocate For Controversial Views In Association With Others.

The First Amendment protects the freedom to associate and express political views as a group. *NAACP v. Alabama*, 357 U.S. at 460-62. This right is intertwined with the right to freedom of expression, and "like free speech, lies at the foundation of a free society." *Buckley v. Valeo*, 424 U.S. 1, 25 (1976) (quoting *Shelton v. Tucker*, 364 U.S. 479, 486 (1960) (internal quotation omitted)). This constitutional protection is critical because "[e]ffective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association[.]" *NAACP v. Alabama*, 357 U.S. at 460; *Bates v. City of Little Rock*, 361 U.S. 516, 522-23 (1960) (the Constitution protects freedom of association to encourage the "advancing ideas and airing grievances"). As is set forth in Movant's declaration, Movant uses Internet forums targeted by the subpoenas, including Twitter and The Right Stuff website, to engage in online political activism and advocacy in concert with like-minded individuals - precisely the sort of activity at the heart of the First Amendment's protections.

The Supreme Court has repeatedly held that compelled disclosure of an advocacy group's membership lists harms freedom of association because "it may induce members to withdraw from the association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of their exposure." *NAACP v. Alabama*, 357 U.S. at 462-63. *See also Bates*, 361 U.S. at 523; *Gibson v. Florida Legislative Investigation Comm.*, 372 U.S. 539 (1963). This rule applies with equal force to attempts to compel disclosure of information usable to reveal Movant's identity here.

Anonymity in one's associational ties is closely linked to freedom of association, particularly where, as here, individuals associate to advocate dissident views: "Inviolability of privacy in group association may in many circumstances be indispensible to preservation of freedom of association, particularly where a group espouses dissident beliefs." *NAACP v. Alabama,* 357 U.S. at 462. Here, Plaintiffs seek all non-public direct messages associated with Movant's Twitter account (as well as the Twitter accounts of untold thousands of others), including direct messages exchanged with Twitter accounts with which Movant associates for the purpose of political activism and advocacy. Plaintiffs also seek all other data associated with those Twitter accounts, including Movant's, including non-public email addresses, location data, and telephone numbers[25] - information that is potentially personally identifying. Plaintiffs also seek IP addresses and MAC addresses in traffic logs for websites visited by Movant, which data is usable to not only identify Movant and the ISP's Movant uses, but is also usable to map Movant's location over time. Such location data includes a wealth of details about one's habits and day-to-day patterns, which are intimately tied to one's associational activities. *United States v. Jones*, 132 S. Ct. 945,

[25] See Doc. 226-2 at 4-5, seeking all account data and https://help.twitter.com/en/managing-your-account#username-email-and-phone (showing that email and telephone data are typically associated with Twitter accounts).

954 (2012) (Sotomayor, J., concurring) (continual location monitoring over a prolonged period "reflects a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."). As the D.C. Circuit has noted, such observation of a person's movements

> reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. . . . A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S.Ct. 945.

Plaintiffs' other subpoenas are aimed squarely at identifying and mapping the movements of individuals involved in political expression and association: specifically, political expression on issues of race and identity. The Court (and indeed the average American) may well disagree with the substance of this expression and the goals of associations of individuals engaged in it. Nevertheless, Movant, and ideological fellow travelers, have a right to "engage in association for the advancement of beliefs and ideas," and discovery tending to chill that association is therefore subject to heightened scrutiny. *NAACP v. Alabama*, 357 U.S. at 460.

b. Movant Has A Qualified First Amendment Privilege In Associational Privacy Requiring A Heightened Showing Of Relevance To Overcome.

"The First Amendment [] establishes the right to associate with others and organize in protest… It applies in the context of discovery as a qualified privilege against disclosure of information when the party asserting the privilege demonstrates that the disclosure would likely

impair the associational activities of the group." *Marfork Coal Co. v. Smith*, 274 F.R.D. 193, 205, 2011 WL 1044496 (S.D.W. Va. 2011) (denying discovery request directed to defendant environmental advocacy organization's member list); *NAACP v. Alabama*, 357 U.S. at 460-63; *Perry*, 591 F.3d at 1140; *In re Motor Fuel Temperature Sales Practices Litig.*, 641 F.3d 470, 481 (10th Cir. 2011) (First Amendment privilege protects rights of association affected by civil discovery demands). When discovery requests infringe upon political expression and association, the courts apply heightened discovery standards to protect those constitutional values. *Perry,* 591 F.3d at 1140; *Fed. Election Comm'n v. Larouche Campaign*, 817 F.2d 233, 234-35 (2d Cir. 1987) (requiring agency to demonstrate need beyond mere relevance to an investigation to justify compelling disclosure of the names of campaign contributors).

The Supreme Court has made clear that infringements on freedom of association may survive constitutional scrutiny only when they "serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms." *Roberts v. United States Jaycees*, 468 U.S. 609, 623 (1984); *see also NAACP v. Button*, 371 U.S. at 341; *Knox v. SEIU, Local 1000*, 132 S. Ct. 2277, 2291 (2012) (burden on freedom of association "must serve a compelling interest and must not be significantly broader than necessary to serve that interest.").

To make a prima facie showing that the privilege applies, a party must "demonstrate an objectively reasonable probability that compelled disclosure will chill associational rights, i.e., that disclosure will deter membership due to fears of threats, harassment, or reprisal ... which may affect members' physical wellbeing, political activities or economic interests." *In re Motor Fuel*, 707 F. Supp. at 1153. "To demonstrate an objectively reasonable probability of a chilling effect, the party asserting the privilege does not need to prove to a certainty that disclosure will result in

chilling. Instead, the party 'need only show that there is some probability that disclosure will lead' to a chilling effect." *Pulte Home Corp. v. Montgomery Country Maryland*, No. GJH-14-3955, 2017 WL 1104670 at *4 (D. Maryland March 24, 2017) quoting *Black Panther Party*, 661 F.2d at 1268. Declarations are sufficient to make this showing. *Perry,* 591 F.3d at 1143.

i. There Is A High Probability That Movant's Associational Rights Will Be Curtailed By The Requested Discovery.

As Movant's declaration filed with this motion demonstrates, the disclosure of Movant's identity, Movant's non-public communications, and Movant's association with the "alt-right" and right wing ideas and people is likely to result in harassment, Movant's withdrawal from right wing online advocacy and activism, and a chilling of Movant's political expression. Doe. Decl. at ¶14. These impacts will also likely be felt by the thousands of other individuals whose personal data is targeted by Plaintiffs' subpoenas. As is discussed in IV(A)(1)(b) *supra*, being "doxed" as "alt-right" has severe personal and professional consequences, up to and including risk of physical assault. Even without these sorts of severe consequences, the associational chilling effect of compelled disclosure of personal information is a matter of "common sense". As Magistrate Judge Sullivan noted just last year in *Pulte Home Corp.*,

> If a person knows that her communications will be disclosed to an unintended audience in the future, she may be more cautious in her statements or refrain from speaking entirely. In the same way, a person who belongs to a group that is required to disclose its internal communications in civil litigation may decide that the invasiveness of the disclosure outweighs the benefit of belonging to or participating in the group.

Pulte Home Corp., 2017 WL 1104670 at *8.

And again, the goal of this entire lawsuit, from the standpoint of Plaintiffs' counsel at least, is to "make racists afraid again." See IV(A)(1)(c)(i) *supra*. Plaintiffs' cannot now be heard to say that their efforts in spreading fear among "racists" are not likely to be successful.

Accordingly, Movant has made a *prima facie* showing production of the data sought by Plaintiffs' subpoenas will chill Movant's and others' constitutionally protected associational rights.

ii. Plaintiffs Cannot Meet The Heightened Showing Of Relevance Required To Overcome Movant's First Amendment Privilege In Private Associations.

Once movant has established the risk of chilling of associational rights, the burden then shifts to the discovery proponent to show that the discovery is proper. See *Pulte Home Corp.*, 2017 WL 1104670 at *4. In *Pulte Home Corp.*, the court considered the proper balancing test to apply when weighing discovery requests directed at non-parties, which were likely to chill associational rights. Magistrate Judge Sullivan synthesized the various articulations of the balancing test found in *Grandbouche*, *Perry*, *Black Panther Party* and *Marfork* into a four factor test, which considers:

1. The relevance of the information sought and whether it is of central or crucial importance to the case;

2. The necessity of the information sought and whether it is sought for improper ulterior motives;

3. The availability of the information from alternative sources, and

4. The substantiality of the First Amendment interests at stake.

Pulte Home Corp., 2017 WL 1104670 at *9 citing *Perry*, *Grandbouche* and *The Black Panther Party*.

The Court should apply this articulation of the balancing test here. Under this test, it is clear that Plaintiffs' cannot show entitlement to the requested discovery. As is set forth *supra* in section IV(A)(1)(c)(ii), the information sought, considering the breadth of the subpoenas, is not crucial or central to Plaintiffs' case, which is that the named Defendants' conspired to incite

violence at Charlottesville. As is set forth *supra* in section IV(A)(1)(c)(i), the subpoenas are not motivated by their necessity to Plaintiffs' case, but rather, by an improper and ulterior motive - to discourage political speech and association among the "alt-right". As is set forth supra in section IV(A)(1)(c)(iii), the discovery that is actually relevant to Plaintiffs' case is available through conventional party discovery requests directed at the Defendants. As to the substantiality of the First Amendment interests at stake, what is at stake is the chilling of political association and political speech among dissidents by subjecting individuals to loss of employment, loss of family ties and possible physical assault. The First Amendment interests here could not be more fundamental. Plaintiffs' requests fail the balancing test, and their subpoenas should be quashed in their entirety.

c. The Hatreon Subpoena Must Be Quashed Because It Trammels First Amendment Associational Rights.

The First Amendment rights to anonymous association and speech discussed above have also been found to include the right to anonymously fund political advocacy under circumstances similar to those here. In *Brown v. Socialist Workers '74 Campaign Comm. (Ohio)*, 459 U.S. 87, 101–02, (1982), the Court found a First Amendment exemption from compliance with state requirements to disclose political party donor lists, because the party was a minor one, and disclosure of its supporters would subject them to private harassment. Justice Thurgood Marshall, writing for the Court, noted,

> The First Amendment prohibits a state from compelling disclosures by a minor party that will subject those persons identified to the reasonable probability of threats, harassment or reprisals. Such disclosures would infringe the First Amendment rights of the party and its members and supporters.

Id. This principle prevents enforcement of the Hatreon subpoena[26], which is directed to uncovering the all communications with and identities of every individual who has donated money through Hatreon to one of the Defendants or 50 other individuals. See Doc. 226-5 at 9. Doxing these individuals would subject them to same sort of private harassment suffered by party supporters in *Brown*, which impermissibly interferes with their First Amendment right to association.

B. The Twitter and Hatreon Subpoenas Must Be Quashed Pursuant to 18 U.S.C. §2702(a)

The Twitter and Hatreon subpoenas seek electronic communications held in storage by those third-parties. Specifically, Request No. 7 in the Twitter subpoena seeks all communications between and among Primary Users and Secondary Users, and Request No. 6 seeks identification of Secondary User accounts, where "accounts" is defined to include all communications associated with the account, even non-public direct messages. Doc. 226-2 at 4-5 and 9. The Hatreon subpoena similarly seeks electronic communications. Doc. 226-8 at 8 (Request Nos. 1 & 3). These communications cannot be produced by Twitter or Hatreon pursuant to federal statute.

The Stored Communications Act (18 U.S.C. §2701 et seq.) prohibits the release of stored electronic communications in response to a civil subpoena. Specifically, 18 U.S.C. §2702(a)(1)

---

[26] If the Court determines that Movant lacks standing to challenge the Hatreon subpoena, it should still quash it *sua sponte*. See *Jefferson*, 2012 WL 1150415, at *2; *Newcomb.*, 2008 WL 3539520 at *3 (regarding the court's inherent power to *sua sponte* quash improper subpoenas).

provides "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service". Similar prohibitions against the release of ephemerally stored electronic communications are set forth in §2702(a)(2). Twitter and Hatreon may be civilly liable if they comply with their subpoenas. 18 U.S.C. §2707 (conferring standing on any "subscriber, or other person aggrieved by any violation of this chapter" to bring a private action for violations)[27]. As this Court's sister court has noted, the plain language of §2702 prohibits enforcement of a civil subpoena that seeks the production of electronically stored communications. *In re Subpoena Duces Tecum to AOL, LLC*, 550 F.Supp.2d 606, 611-612 (E.D. Va. 2008). Thus, the Twitter and Hatreon subpoenas should be quashed on this basis, independent of the constitutional issues raised above.

C. The Subpoenas Are Overbroad, Burdensome And Disproportional And Should Be Quashed In Their Entirety

Constitutional and statutory issues aside, the Court should quash all four subpoenas because they violate the Federal Rules. Fed. R. Civ. P. 45(d)(3)(A)(iv) *requires* a court to quash a subpoena that "subjects a person to undue burden". "A [third-party] subpoena imposes an undue burden on a party when a subpoena is overbroad." *In re Subpoena Duces Tecum to AOL, LLC*, 550 F.Supp.2d at 612 citing *Theofel*, 359 F.3d at 1071–72. Thus, a party has standing to challenge a third-party subpoena that is overbroad, and therefore unduly burdensome. As a sister court has noted, "it is the practice and precedent in this district that parties enjoy the right to challenge subpoenas directed at third parties on the basis of undue burden. *In re Subpoenas for Documents Issued to ThompsonMcMullan, P.C.*, No. CV 3:16-MC-1, 2016 WL 1071016, at *4

[27] Indeed, Plaintiffs *and their counsel* may be civilly liable if Twitter and Hatreon comply with their subpoenas. See *Theofel v. Farey-Jones*, 359 F.3d 1066, 1079 (9th Cir. 2004).

(E.D. Va. Mar. 17, 2016) citing *Singletary v. Sterling Transport Co., Inc.*, 289 F.R.D. 237, 239, 240 n.2 (E.D. Va. 2012). This standing should be extended to third-parties such as Movant where, as here, Movant's personal information stands at risk of disclosure. Indeed, the Rules suggest as much. Rule 26(c) permits the Court to enter a protective order protecting "a party or person from annoyance, embarrassment, oppression, or undue burden or expense". The "person" of Rule 26(c) can be anyone burdened, annoyed, embarrassed or oppressed by the discovery. Accordingly, Movant has standing to object to an overbroad subpoena, relating to Movant's information, served on third parties such as those here. See *In re Subpoenas for Documents Issued to ThompsonMcMullan*, 2016 WL 1071016, at *4 (discussing the interplay between Rules 45 and 26(b) and adopting a "pragmatic approach" to standing to challenge third party subpoenas.)

Whether a subpoena issued under Rule 45 is overbroad is determined according to the relevancy standards of Rule 26(b). *Anker v. G.D. Searle & Co.*, 126 F.R.D. 515, 518 (M.D.N.C. 1989). But "[i]n the context of evaluating subpoenas issued to third parties, a court 'will give extra consideration to the objections of a non-party, non-fact witness in weighing burdensomeness versus relevance.'" *Schaaf v. SmithKline Beecham Corp.*, 233 F.R.D. 451, 453 (E.D.N.C. 2005) quoting *Indem. Ins. Co. of N. Am. v. Am. Eurocopter LLC*, 227 F.R.D. 421, 426 (M.D.N.C.2005). This heightened relevancy requirement requires that third party subpoenas be narrowly tailored to avoid sweeping up irrelevant information. In granting a motion to quash third party subpoenas as overbroad under Rule 26(b), a court in the Eastern District of Virginia explained,

> Put another way, any [third party] subpoena that seeks evidence that is neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, or that is so overbroad that compliance with its demands will necessarily require

> production of irrelevant evidence, seeks evidence outside the scope of Rule 26(b)(1).

In re Subpoenas for Documents Issued to ThompsonMcMullan, 2016 WL 1071016, at *5. Another Eastern District court quashed a third-party subpoena for party email communications for being overbroad because it did not impose parameters limiting the subpoena's scope to evidence relevant in the underlying litigation:

> Similar to the subpoena in *Theofel*, State Farm's subpoena must be quashed because it imposes an undue burden on the Rigsbys by being overbroad and requesting "all" of Cori Rigsby's e-mails for a six-week period. Like the subpoena in *Theofel*, State Farm's subpoena is overbroad because it does not limit the e-mails requested to those containing subject matter relevant to the underlying action or sent to or from employees connected to the litigation, other than Cori Rigsby.

In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 612, 2008 WL 1956266 (E.D. Va. 2008). *Theofel v. Farey-Jones*, 359 F.3d 1066, 1071-72 (9th Cir. 2004) stands for a similar proposition. In that case, plaintiff's counsel sent a subpoena to defendant's email host, demanding all of defendant's emails, without limiting the scope of the subpoena temporally or to the subject matter of the underlying litigation. *Theofel*, 359 F. 3d at 1071. The district court and then the Ninth Circuit roundly castigated plaintiff's counsel. *Id.* ("One might have thought... that the subpoena would request only e-mail related to the subject matter of the litigation, or maybe messages sent during some relevant time period, or at the very least those sent to or from employees in some way connected to the litigation.").

Plaintiffs' requests are clearly overbroad, and therefore unduly burdensome, in view of these standards. As is set forth *supra*, the Twitter subpoena seeks communications between and among Primary and Secondary Users, *on any subject whatsoever*, as well as all communications involving Secondary Users (including non-public direct messages) with any party, on any subject. The Secondary Users are not defendants in this litigation, and probably number in the

high tens of thousands. The Hatreon subpoena seeks all communications regarding donations from anyone to anyone on a list of over 50 non-Defendant individuals. Doc. 226-5 at 4-5 (defining "Other Relevant Individuals"). The traffic logs sought from Cloudflare and Godaddy will include IP and MAC addresses for likely tens of thousands of people unrelated to this litigation. The subpoenas fails to impose parameters limiting their scope to evidence relevant in the underlying litigation, and they must therefore be quashed.

What's more, all of the opinions cited *supra* regarding the heightened relevancy burden for third party subpoenas were decided in cases brought before the proportionality requirement was added to narrow the scope of discovery under Rule 26(b). Under the amended rule, discoverable information must be both relevant and

> proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

Fed. R. Civ. P. 26(b)(1). The subpoenas fail the proportionality test too. To the extent that there are relevant needles buried in the haystack sought by Plaintiffs, the burden of production outweighs the benefit, and the discovery sought has little importance to the issues of the case. And it difficult to see how this voluminous discovery is justified in view of the importance of the issues at stake in this action[28].

Alternatively or additionally, the Court should enter a protective order pursuant to Fed. R. Civ. P. 26(c) preventing enforcement or compliance with the subpoenas. See *Brown v.*

---

[28]While Movant does not wish to trivialize the physical or emotional injuries of the Plaintiffs described in their complaint, it is important to remember that this is not a wrongful death suit.

Mountainview Cutters, LLC, No. 7:15-CV-00204, 2016 WL 3045349, at *2 (W.D. Va. May 27, 2016) (finding that a party lacking standing under Rule 45 to quash a third party subpoena may still challenge the subpoena under Rule 26(b) and receive a protective order under Rule 26(c). For the reasons set forth above, the Court should enter a protective order preventing enforcement or compliance with these shorts of overbroad third party discovery requests, both now and in the future.

V. CONCLUSION

The subpoenas, and the lawsuit on which they are based, are aimed at preventing Americans who espouse far-right political ideas from engaging in free speech and free association by subjecting people who have done no wrong to embarrassment, loss of employment, social ostracism and possibly even threats of physical harm. The Court likely finds the ideals held by the "alt-right" to be repugnant. Most Americans do. But the First Amendment exists precisely to safeguard the right to express and advocate for controversial ideas with which the majority disagrees. After all, no such protections are necessary when one is expressing popular ideas consistent with prevailing orthodoxy.

And it is vital to understand the dangers here. This will not stop with the "alt-right". If allowed, Plaintiffs' tactics will quickly be applied to other groups. One can easily imagine lawsuits supporting third-party requests to identify everyone who is member of the Mosque attended by Omar Mateen, the Islamic terrorist who killed 49 people in Orlando, Florida in 2016[29], or everyone involved in the Black Lives Matter movement, which inspired the murders

[29] See https://en.wikipedia.org/wiki/Orlando_nightclub_shooting

of 8 police officers by Gavin Long and Micah Johnson in 2016[30], or the donors to the Southern Poverty Law Center, which provided a map enabling Floyd Corkins to shoot up the Family Research Council in 2012[31]. The Court should end this now, and protect the First Amendment rights of Movant, and all those similarly situated, of whatever political ideology. For the reasons set forth above, the subpoenas should be quashed.

DATED: February 23, 2018

Respectfully Submitted

John Doe

/s/ John Doe
Pro Se
subpoenadoe1@protonmail.com

[30] See https://en.wikipedia.org/wiki/2016_shooting_of_Baton_Rouge_police_officers#Victims; https://en.wikipedia.org/wiki/2016_shooting_of_Dallas_police_officers
[31] See https://www.cnn.com/2012/08/16/us/dc-shooting-blame/index.html

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of February, 2018, a copy of the foregoing was submitted to the Clerk's office of the Charlottesville Division of the U.S. District Court for the Western District of Virginia at 255 W. Main Street, Room 304, Charlottesville, VA 22902 by U.S. Postal Service Express Mail. A copy of this submission was sent by email to the email addresses of the parties and counsel listed below.

/s/ John Doe
Pro Se

pbowman@bsfllp.com (attorney for Plaintiffs)
rcahill@cooley.com (attorney for Plaintiffs)
ybarkai@bsfllp.com (attorney for Plaintiffs)
dcampbell@dhdglaw.com (attorney for Defendant Fields)
kdunn@bsfllp.com (attorney for Plaintiffs)
jfink@kaplanandcompany.com (attorney for Plaintiffs)
jgravatt@dhdglaw.com (attorney for Defendant Fields)
cgreene@kaplanandcompany.com (attorney for Plaintiffs)
wisaacson@bsfllp.com (attorney for Plaintiffs)
bryan@bjoneslegal.com (attorney for Defendant League of the South)
rkaplan@kaplanandcompany.com (attorney for Plaintiffs)
alevine@cooley.com (attorney for Plaintiffs)
jlibling@bsfllp.com (attorney for Plaintiffs)
dmills@cooley.com (attorney for Plaintiffs)
sstrohmeier@kaplanandcompany.com (attorney for Plaintiffs)
isuecrooks@comcast.net (attorney for Defendant Parrott)